UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S):	Stuart S. Kreitzer	GROUP ART UNIT:	2135
APPLN. NO.:	10/631,370	EXAMINER:	Klimach, Paula W
FILED:	July 31, 2003	Confirmation No.	2130
TITLE:	METHOD AND APPARATUS FOR SECURE COMMUNICATIONS AMONG PORTABLE COMMUNICATION DEVICES		

CERTIFICATE UNDER 37 CFR 1.8(a)	
I hereby certify that this correspondence is being electronically transmitted on the date listed below:	
Date:	August 24, 2007
Signature	/Larry G. Brown/
Typed or printed name:	Larry G. Brown

AMENDMENT

Mail Stop: **AMENDMENT**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This communication is responsive to the Office Action mailed March 20, 2007 relating to the above-identified application. A three-month Extension of Time is being paid concurrently with this submission.

The Commissioner is hereby authorized to charge any requisite fees to Motorola, Inc. Deposit Account No. 502117.

Amendments to the Claims begin on page 2 of this paper.

Remarks/Arguments begin on page 12 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) A method of establishing secure communications in a multi-mode portable communication device, comprising the steps of:

establishing a symmetric traffic key between the multi-mode portable communication device and a second multi-mode portable communication device in a first mode of communication in a first communication network that supports a first communication protocol;

switching to at least a second mode of communication in a different communication network that supports a different communication protocol; and

following the switch, sharing the symmetric traffic key between the multi-mode portable communication device and the second multi-mode portable communication device;

wherein the multi-mode device and the second multi-mode device communicate with one another using the first communication protocol over the first communication network and using the different communication protocol over the different communication network.

2. (previously presented) The method of claim 1, wherein the step of establishing the symmetric traffic key is achieved using Automatic Public Key exchange techniques by having the multi-mode portable communication device and the second portable communication device each independently computing the symmetric traffic key using their respective private keys along with a public key of a peer unit before commencing secure communications in a first mode.

3. (original) The method of claim 2, wherein the Automatic Public Key exchange is implemented using public-key algorithms such as Diffie-Hellman cryptography or Elliptic Curve Cryptography.

4. (original) The method of claim 3, wherein the Automatic Public Key exchange is implemented by combining public-key algorithms with a signaling scheme such as Future Narrow Band Digital Terminal protocol.

5. (previously presented) The method of claim 1, wherein the step of switching to the second mode from the first mode comprises switching among modes comprising interconnect voice, dispatch voice, peer-to peer data, and peer-to-peer voice.

6. (previously presented) The method of claim 1, wherein the step of switching to the second mode from the first mode comprises switching among communication protocols comprising CDMA, TDMA, GSM, and WLAN.

7. (previously presented) The method of claim 1, wherein the method further comprises the step of storing the symmetric traffic key in a phonebook record associated with the second portable communication device or storing the symmetric traffic key in a recent call list that reflects recent communications between the multi-mode portable communication device and the second portable communication device.

8. (canceled)

9. (original) The method of claim 1, wherein the method further comprises the step of establishing a new communication session between the multi-mode portable communication device and the second portable communication device without requiring an APK key establishment process.

10. (previously presented) The method of claim 1, wherein the method further comprises the step of establishing a key exchange with a plurality of other predetermined portable communication devices during an idle mode.

11. (currently amended) A method of establishing secure communications among a plurality of multi-mode portable communication devices, comprising the steps of:

storing information associated with a predetermined number of other multi-mode portable communication devices;

establishing a symmetric traffic key using an APK key establishment process between a first multi-mode portable communication device and the predetermined number of other multi-mode portable communication devices during an idle mode of the first multi-mode portable communication device;

establishing a secure communication session in a first mode of communication in a first communication network that supports a first communication protocol between the first multi-mode portable communication and at least one among the predetermined number of other multi-mode portable communication devices without further requiring the APK key establishment process;

switching to at least a second mode of communication in a second communication network that is different from the first communication network and that supports a second communication protocol that is different from the first communication protocol; and

following the switch, sharing the symmetric traffic key between the first multi-mode portable communication device and the at least one among the predetermined number of other multi-mode portable communication devices in the second type of communication;

wherein the first multi-mode device and the other multi-mode device communicate with one another using the first communication protocol over the first

communication network and using the second communication protocol over the second communication network.

12. (original) The method of claim 11, wherein the step of establishing a symmetric traffic key using the APK key establishment process comprises contacting the predetermined number of other portable communication devices to determine if their respective keys have expired and performing a background APK exchange to re-establish a fresh key if the respective key has expired.

13. (canceled)

14. (currently amended) A portable communication device capable of operating in multiple modes, comprising:

a transceiver;

a processor coupled to the transceiver, wherein the processor is programmed to:

establish a symmetric traffic key in a first mode of communication in a first communication network that supports a first communication protocol between the multi-mode portable communication device and a second multi-mode portable communication device;

switch to at least a second mode of communication in a different communication network that supports a different communication protocol;

following the switch, share the symmetric traffic key between the multi-mode portable communication device and the second multi-mode portable communication device;

wherein the multi-mode device and the second multi-mode device communicate with one another using the first communication protocol over the first communication network and using the different communication protocol over the different communication network.

15. (original) The portable communication device of claim 14, wherein the processor is programmed to establish the symmetric traffic key using Automatic Public Key exchange techniques.

16. (original) The portable communication device of claim 15, wherein the Automatic Public Key exchange is implemented using a signaling scheme such as Future Narrow Band Digital Terminal protocol combined with public-key algorithms such as Diffie-Hellman cryptography or Elliptic Curve Cryptography.

17. (previously presented) The portable communication device of claim 14, wherein the processor is programmed to switch to the second mode from the first mode by switching among modes comprising interconnect voice, dispatch voice, peer-to peer data, peer-to-peer voice, or by switching among communication protocols comprising CDMA, TDMA, GSM, and WLAN.

18. (original) The portable communication device of claim 14, wherein the processor is further programmed to store the symmetric traffic key in at least one among a phonebook record associated with the second portable communication device and a cache memory associated with a predetermined number of other portable communication devices in recent secure communication with the portable communication device.

19. (original) The portable communication device of claim 14, wherein the processor is further programmed to establish a new communication session between the portable communication device and the second portable communication device without requiring an APK key establishment process.

20. (previously presented) The portable communication device of claim 14, wherein the processor is further programmed to establish a key exchange with a plurality of other predetermined portable communication devices during an idle mode.

21. (currently amended) A portable communication device capable of operating in multiple modes, comprising:

a transceiver;

a processor coupled to the transceiver, wherein the processor is programmed to:

store information associated with a predetermined number of other multi-mode portable communication devices;

establish a symmetric traffic key using an APK key establishment process between a first multi-mode portable communication device and the predetermined number of other multi-mode portable communication devices during an idle mode of the first multi-mode portable communication device;

establish a secure communication session in a first mode of communication in a first communication network that supports a first communication protocol between the first multi-mode portable communication and at least one among the predetermined number of other multi-mode portable communication devices without further requiring the APK key establishment process;

switch to at least a second mode of communication in a second communication network that supports a second communication protocol; and

following the switch, share the symmetric traffic key between the first multi-mode portable communication device and the at least one among the predetermined number of other multi-mode portable communication devices in the second mode of communication;

wherein the first multi-mode device and the other multi-mode device communicate with one another using the first communication protocol over the first

communication network and using the second communication protocol over the second communication network.

REMARKS/ARGUMENTS

Claims 1-7, 9-12 and 14-21 remain pending in the application, as claims 8 and 13 were previously canceled without prejudice. In the Office Action, claims 1, 6, 10, 14, 18 and 20 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,390,252 to Suzuki (Suzuki) in view of U.S. Patent No. 6,278,697 to Brody (Brody). Claim 7 was rejected under 35 U.S.C. 103(a) as being unpatentable over Suzuki in view of Brody and further in view of U.S. Patent No. 6,965,674 to Whelan, et al. (Whelan). Claims 2, 3, 9, 11, 12, 15, 19 and 21 were rejected under 35 U.S.C. 103(a) as being unpatentable over Suzuki in view of Brody and further in view of Schneier, *Applied Cryptography* (Schneier). Claims 4, 5 and 16 were rejected under 35 U.S.C. 103(a) as being unpatentable over Suzuki in view of Brody in view of Schneier and further in view of the article by L-3 Communications. Finally, claim 17 was rejected under 35 U.S.C. 103(a) as being unpatentable over Suzuki in view of Brody and further in view of the FNBDT Signaling Plan and the L-3 Communications article.

Independent claim 1 has been amended to clarify that the second device is a multi-mode device. This claim has also been amended to clarify that the multi-mode device and the second multi-mode device communicate with one another using the first communication protocol over the first communication network and using the different communication protocol over the different communication network. Claims 11, 14 and 21 have been similarly amended. Support for the amendments can be found in paragraphs 0017 and 0020. No new matter has been added in view of these amendments.

As previously noted in an earlier response, Suzuki does not describe the first mode of communication in a first network and protocol and the second mode of communication in a different network and protocol. Suzuki merely contemplates switching between different channels, i.e., frequencies in the same communication network (see col. 5, lines 38-45), to which the Examiner has agreed (see page 3, lines 4-7 of the Non-Final Office Action of March 20, 2007).

Moreover, Applicants note that Brody describes conducting a communication between a first device operating on a first network using a first protocol and a second device operating on a second network using a second protocol (see col. 3, lines 20-57). This description is in direct contrast with the claimed subject matter of the present application. In fact, if the communication devices were able to conduct calls in which both devices used the same network and protocol for a first call and a second same network and protocol subsequently, then the protocol conversion of Brody, which is the heart of that invention (see col. 3, lines 53-57), would be completely inapplicable.

In view of the above, Applicant submits that the above claims are patentable over the prior art. Reconsideration and withdrawal of the rejection of the claims is respectfully requested. Passing of this case is now believed to be in order, and a Notice of Allowance is earnestly solicited.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim, unless Applicant has argued herein that such amendment was made to distinguish over a particular reference or combination of references.

In the event that the Examiner deems the present application non-allowable, it is requested that the Examiner telephone the Applicant's attorney or agent at the number indicated below so that the prosecution of the present case may be advanced by the clarification of any continuing rejection.

The Commissioner is hereby authorized to charge any necessary fee, or credit any overpayment, to Motorola, Inc. Deposit Account No. 50-2117.

Respectfully submitted,

Date: August 24, 2007

By: /Larry G. Brown/
Larry G. Brown

SEND CORRESPONDENCE TO:

Motorola, Inc.
Law Department – MD 1610
8000 W. Sunrise Blvd.
Plantation, FL 33322

Customer Number: 24273

Attorney of Record
Reg. No.: 45,834

Tel: 954-723-4295 direct line
Tel: 954-723-6449 main line
Fax No.: (954) 723-3871